UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/880,701	06/13/2001	Lee P. Noehring	4224-10US1	5538

29974 7590 12/15/2004

GAMMAGE & BURNHAM, PLC
c/o PortfolioIP
P.O. BOX 52050
Minneapolis, MN 55402

EXAMINER	
PARTHASARATHY, PRAMILA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 12/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/880,701	NOEHRING ET AL.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 October 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *6/13/01 & 9/15/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on 04/03/2003. Claims 1 – 42 were received for consideration. No preliminary amendments to the specification were filed. Claims 1 – 42 are currently being considered.

Claim Objections

2. Claim 8 is objected to because of the following informalities: Claim 8 recites " .... receiving at a context PAM (308), ...". Replace "PAM (308)" with "RAM (308)".

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1- 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baker (U.S. Patent Number 5,948,080, hereinafter "Baker") in view of Krishna et al. (U.S. Patent Number 6,477,646, hereinafter "Krishna").

Regarding Claim 1, Baker discloses a security data packet processing system comprising:

a transmitting (Tx) direct memory access (DMA) interface (314) receiving a streamed security data packet, selecting channel for processing the streamed security data packet and transferring the streamed security data packet to an external memory (Baker Column 5 lines 14 – 54 and Column 10 lines 36 – 63);

an input DMA engine (306) retrieving portions of the streamed security data packet from the external memory after all portions of the streamed security data packet have been transferred to the external memory (Baker Column 5 line 36 – Column 7 line 50 and Column 10 line 36 – 63);

an input FIFO (308) receiving the portions of the streamed security data packet from the input DMA engine (306) in blocks of a predetermined byte size, portions being retained in a portion of the input FIFO allocated to the selected channel (Baker Column 8 line 11 – Column 9 line 15 and Column 17 lines 11 – 35);

a context RAM (308) receiving a security association database (SAD) entry associated with the selected channel, the SAD entry being retrieved from the external memory by the input DMA engine (Baker Column 20 line 24 – 67); and

an input crypto DMA engine (310) providing the blocks of the security data packet processing engine for processing (Baker Column 11 lines 15 – 27; Column 13 lines 6 – 58 and Column 13 line 33 – Column 14 line 10).

Baker does not explicitly disclose that the data packet is a security data packet. However, Krishna discloses an architecture for a cryptography accelerator that allows

significant performance improvements IPSec processing wherein packets are received and processed though DMA (Krishna Column 4 line 34 – Column 6 line 56). Packet processing were well known in the art at the time the invention was made, and its implementation, such as detailed by Baker, in conjunction with the teachings of Krishna would have been obvious to one of ordinary skill in the art at the time the invention was made because if IPSec is processed as taught by Krishna were to be removed, a cryptographic DMA would be needed in order to process the IPSec packets. The addition of such DMA would add and improve the accelerated processing of IP security packets. Therefore it would have been obvious to one of ordinary skill in the art to combine the teachings of Krishna and Baker to add flexibility to process IPSec packets through DMA to improve the speed of processing.

Regarding Claim 8, Baker teaches and describes a method for processing security data packet comprising:

receiving a streamed security data packet (Baker Column 5 lines 14 – 54 and Column 10 lines 36 – 63);

selecting a channel for processing the streamed security data packet;

transferring the streamed security data packet an external memory (Baker Column 5 lines 14 – 54 and Column 10 lines 36 – 63);

retrieving portions the streamed security data packet from the external memory after all portions of the streamed security data packet have been transferred to the

external memory (Baker Column 5 line 36 – Column 7 line 50 and Column 10 line 36 – 63);

transferring the portions of the streamed security data packet an input FIFO (308) from an input DMA engine (306) in blocks of a predetermined byte size, portions being retained portion of the input FIFO allocated to the selected channel (Baker Column 8 line 11 – Column 9 line 15 and Column 17 lines 11 – 35);

receiving a context RAM (308), a security association database (SAD) entry associated with the selected channel, the SAD entry being retrieved from the external memory by the input DMA engine (Baker Column 20 line 24 – 67); and

providing to an input crypto DMA engine (310) the blocks of the security data packet a processing engine for processing (Baker Column 11 lines 15 – 27; Column 13 lines 6 – 58 and Column 13 line 33 – Column 14 line 10).

Baker does not explicitly disclose that the data packet is a security data packet. However, Krishna discloses an architecture for a cryptography accelerator that allows significant performance improvements IPSec processing wherein packets are received and processed though DMA (Krishna Column 4 line 34 – Column 6 line 56). Packet processing were well known in the art at the time the invention was made, and its implementation, such as detailed by Baker, in conjunction with the teachings of Krishna would have been obvious to one of ordinary skill in the art at the time the invention was made because if IPSec is processed as taught by Krishna were to be removed, a cryptographic DMA would be needed in order to process the IPSec packets. The addition of such DMA would add and improve the accelerated processing of IP security

packets. Therefore it would have been obvious to one of ordinary skill in the art to combine the teachings of Krishna and Baker to add flexibility to process IPSec packets through DMA to improve the speed of processing.

Regarding Claim 15, Baker teaches and describes a method of processing an IPSec security protocol packet, the IPSec security protocol packet comprising an IPSec header, the method comprising:

buffering an IPSeC security protocol packet an external memory; reading portions of the buffered IPSeC security protocol packet into a first local buffer, the portions having a predetermined number of bytes; verifying header information of the IPSec security protocol packet (Baker Column 5 lines 14 – 54 and Column 10 lines 36 – 63);

reading a security association database (SAD) entry into the first local buffer; processing the IPSec security protocol packet based on information in the SAD entry; and storing the processed IPsec security protocol packet in an external memory (Baker Column 20 line 24 – 67).

Baker does not explicitly disclose that the data packet is a security data packet. However, Krishna discloses an architecture for a cryptography accelerator that allows significant performance improvements IPSec processing wherein packets are received and processed though DMA (Krishna Column 4 line 34 – Column 6 line 56). Packet processing were well known in the art at the time the invention was made, and its implementation, such as detailed by Baker, in conjunction with the teachings of Krishna

would have been obvious to one of ordinary skill in the art at the time the invention was made because if IPSec is processed as taught by Krishna were to be removed, a cryptographic DMA would be needed in order to process the IPSec packets. The addition of such DMA would add and improve the accelerated processing of IP security packets. Therefore it would have been obvious to one of ordinary skill in the art to combine the teachings of Krishna and Baker to add flexibility to process IPSec packets through DMA to improve the speed of processing.

Regarding Claim 23, Baker teaches and describes an application specific integrated circuit processing IPSec security protocol packets comprising:

a first streaming interface communicating with a network processor over a streaming interface and receiving streamed packet (Baker Column 5 lines 14 – 54 and Column 10 lines 36 – 63);

an input buffer storing portions of the streamed packet along with control information for the packet (Baker Column 5 lines 14 – 54 and Column 10 lines 36 – 63);

a crypto core engine performing IPSec cryptographic operations on the packet accordance with the control information (Baker Column 11 lines 15 – 27; Column 13 lines 6 – 58 and Column 13 line 33 – Column 14 line 10);

an output buffer storing processed portions of the streamed packet (Baker Column 13 lines 1 – 51); and

a second streaming interface receiving the processed portions of the streamed packet from the output buffer and providing the network processor a processed IPSec

packet over the streaming interface (Baker Column 17 lines 11 – 60 and Column 18 lines 24 – 67).

Baker does not explicitly disclose that the data packet is a security data packet. However, Krishna discloses an architecture for a cryptography accelerator that allows significant performance improvements IPSec processing wherein packets are received and processed though DMA (Krishna Column 4 line 34 – Column 6 line 56). Packet processing were well known in the art at the time the invention was made, and its implementation, such as detailed by Baker, in conjunction with the teachings of Krishna would have been obvious to one of ordinary skill in the art at the time the invention was made because if IPSec is processed as taught by Krishna were to be removed, a cryptographic DMA would be needed in order to process the IPSec packets. The addition of such DMA would add and improve the accelerated processing of IP security packets. Therefore it would have been obvious to one of ordinary skill in the art to combine the teachings of Krishna and Baker to add flexibility to process IPSec packets through DMA to improve the speed of processing.

Regarding Claim 26, Baker teaches and describes 26. A method of processing data packets for implementing a security protocol, the method comprising:

receiving at a first streaming interface an IP data packet from a network processor, the IP data packet including a security association database (SAD) tag prepended thereto; moving at least portions of the IP data packet in a first portion of first buffer (Baker Column 5 lines 14 – 54 and Column 10 lines 36 – 63);

reading an SAD entry corresponding to the SAD tag into a second portion of the first buffer; prepending control information the IP data packet (Baker Column 20 line 24 – 67);

processing the IP data packet by performing a cryptographic operation on the IP data packet to generate a security protocol data packet; and streaming the security protocol data packet from a second streaming interface to the network processor for transmission through the network (Baker Column 11 lines 15 – 27; Column 13 lines 6 – 58; Column 13 line 33 – Column 14 line 10 and Column 17 lines 11 – 60).

Baker does not explicitly disclose that the data packet is a security data packet. However, Krishna discloses an architecture for a cryptography accelerator that allows significant performance improvements IPSec processing wherein packets are received and processed though DMA (Krishna Column 4 line 34 – Column 6 line 56). Packet processing were well known in the art at the time the invention was made, and its implementation, such as detailed by Baker, in conjunction with the teachings of Krishna would have been obvious to one of ordinary skill in the art at the time the invention was made because if IPSec is processed as taught by Krishna were to be removed, a cryptographic DMA would be needed in order to process the IPSec packets. The addition of such DMA would add and improve the accelerated processing of IP security packets. Therefore it would have been obvious to one of ordinary skill in the art to combine the teachings of Krishna and Baker to add flexibility to process IPSec packets through DMA to improve the speed of processing.

Claims 2 and 9 are rejected applied as above in rejecting Claims 1 and 8. Furthermore, Baker discloses a security data packet processing system further comprising:

an output crypto FIFO (320) receiving processed blocks the security packet from the processing engine (Baker Column 8 lines 18 – 42; Column 17 lines 11 – 40 and Krishna Column 5 line 51 – Column 6 line 14);

an output DMA engine (322) transferring the processed blocks the security packet to an external output memory (158) (Baker Column 7 lines 40 – 65; Column 17 lines 11 – 62 and Krishna Column 5 line 51 – Column 6 line 42); and

receiving direct memory access (DMA) interface (324) retrieving the processed blocks of the security packet from the external output memory (158) after all portions of the processed security data packet have been transferred to the external output memory (158), and transferring the processed blocks of the security data packet to streaming interface for streaming (Baker Column 25 line 39 – Column 26 line 67 and Krishna Column 6 lines 24 – 56).

Claims 4 and 11 are rejected applied as above in rejecting Claims 1 and 8. Furthermore, Baker discloses a security data packet processing system, wherein the context RAM (308) includes a portion storing program state information associated with the selected channel (Baker Column 7 lines 13 – 65).

Claims 5 and 12 are rejected applied as above in rejecting Claims 1 and 8. Furthermore, Baker discloses a security data packet processing system further comprising selecting a least busy channel based amount of buffer space available for a channel in the external memory (156), the selecting being performed by the transmitting (Tx) DMA interface (314) (Baker Column 12 lines 59 – 67).

Claims 6 and 13 are rejected applied as above in rejecting Claims 1 and 8. Furthermore, Baker discloses a security data packet processing system wherein when the security packet is an outbound IPSeC security packet and wherein an outer header (56) and IPSec header are added to the outbound IPSeC security packet when portions of the packet are buffered in input FIFO (308) (Krishna Column 6 lines 1 – 39 and Column 7 line 63 – Column 8 line 19).

Claims 7 and 14 are rejected applied as above in rejecting Claims 1 and 8. Furthermore, Baker discloses a security data packet processing system wherein when the security packet is an inbound IPSec security packet and wherein an outer header (66) and IPSeC header (65) are removed from the outbound IPSec security packet prior to portions the packet being buffered in input FIFO (308) (Krishna Column 5 line 51 – Column 6 line 11 and Column 7 line 63 – Column 8 line 11).

Claims 3 and 10 are rejected applied as above in rejecting Claims 2 and 9. Furthermore, Baker discloses a security data packet processing system further

comprising storing length information for each of a plurality of processed security data packets in one of a plurality of registers of the receiving (Rx) DMA interface (324), and wherein the receiving (Rx) DMA interface (324) performs the retrieving in response to the storing of the length information for an associated processed security data packet (Krishna Column 6 lines 24 – 42).

Claims 16 and 27 are rejected applied as above in rejecting Claims 15 and 26. Furthermore, Baker discloses a security data packet processing further comprising parsing the IPSec header to retrieve a pointer comprising to the SAD entry (Baker Column 11 lines 15 – 27; Column 13 lines 6 – 58; Column 13 line 33 – Column 14 line 10; Column 20 line 24 – 67 and Krishna Column 4 line 34 – Column 6 line 56).

Claim 17 is rejected applied as above in rejecting Claim15. Furthermore, Baker discloses a security data packet processing wherein prior to the processing step, the method includes prepending control information to the IPSec security protocol packet based on information the SAD entry, the control information for use in the processing step (Baker Column 11 lines 15 – 27; Column 13 lines 6 – 58; Column 13 line 33 – Column 14 line 10; Column 20 line 24 – 67 and Krishna Column 4 line 34 – Column 6 line 56).

Claim 18 is rejected applied as above in rejecting Claim 15. Furthermore, Baker discloses a security data packet processing wherein the processing step includes performing cryptographic operation on the IPSec security protocol packet, the cryptographic operation comprising either a decryption function or an authentication function when the IPSec security protocol packet is an inbound packet, and an encryption operation when the IPSec security protocol packet an outbound packet (Krishna Column 5 line 26 – Column 6 line 14).

Claims 19, 24, 25 and 30 are rejected applied as above in rejecting Claims 15 and 23. Furthermore, Baker discloses a security data packet processing further comprising selecting a least busy channel of a plurality of channels for processing the IPSec security protocol packet, and wherein the external memory has a portion associated with least busy channel (Baker Column 12 lines 59 – 67).

Claim 20 is rejected applied as above in rejecting Claim 15. Furthermore, Baker discloses a security data packet processing wherein after the processing step, the method includes buffering the processed IPSeC security protocol packet a buffer allocated to the channel selected for the packet (Baker Column 17 lines 11 – 60 and Column 18 lines 25 – 67).

Claim 21 is rejected applied as above in rejecting Claim 15. Furthermore, Baker discloses a security data packet processing further comprising performing a security

policy cheek on the processed IPSec security protocol packet, security policy check comprising verifying that an IP source address is within a range of addresses identified by the SAD entry (Baker Column 8 lines 18 – 65 and Column 26 line 63 – Column 27 line 44).

Claim 22 is rejected applied as above in rejecting Claim 15. Furthermore, Baker discloses a security data packet processing further comprising performing an anti-replay check on the processed IPSeC security protocol packet, and updating a current byte count and anti-replay fields of the SAD entry (Baker Column 25 line 58 – Column 26 line 19).

Claim 28 is rejected applied as above in rejecting Claim 27. Furthermore, Baker discloses a security data packet processing wherein the security protocol is an IPSec protocol, and wherein the security header is an IPSec header, and wherein the security protocol data packet is formatted in accordance with an IPSec security protocol (Krishna Column 5 lines 51 – 67).

Claim 29 is rejected applied as above in rejecting Claim 26. Furthermore, Baker discloses a security data packet processing wherein the cryptographic operation comprises either an encryption or authentication cryptographic operation, and wherein the method further comprising storing at least portions of the security protocol data packet in a second buffer (Krishna Column 5 lines 51 – 67).

Claim 31 is rejected applied as above in rejecting Claim 26. Furthermore, Baker discloses a security data packet processing further comprising, prior to the reading, obtaining a semaphore for the SAD entry to prevent modification of data within the SAD entry by other channels (Baker Column 26 line 20 – Column 27 line 44).

Claim 32 is rejected applied as above in rejecting Claim 31. Furthermore, Baker discloses a security data packet processing further comprising, subsequent to the reading, updating a byte count and sequence number in the SAD entry (Baker Column 25 line 39 – Column 27 line 27).

Claim 33 is rejected applied as above in rejecting Claim 26. Furthermore, Baker discloses a security data packet processing wherein the storing comprises buffering the portions of the security protocol data packet, the portions comprising a predetermined number of bytes (Baker Column 8 line 11 – Column 9 line 15 and Column 17 lines 11 – 35).

Claim 34 is rejected applied as above in rejecting Claim 26. Furthermore, Baker discloses a security data packet processing wherein the control information identifies an algorithm and key for the cryptographic operation to apply to the IP data packet (Krishna Column 5 line 51 – Column 6 line 14 and Column 7 line 13 – Column 8 line 35).

Claim 35 is rejected applied as above in rejecting Claim 26. Furthermore, Baker discloses a security data packet processing further comprises checking a path maximum transmission unit (PMTU) value of the IP data packet including the security header and the outer IP header as prepended to the data packet to determine when the PMTU value exceeds a PMTU value for a tunnel through which the security protocol data packet destined (Baker Column 11 lines 15 – 27; Column 13 lines 6 – 58; Column 13 line 33 – Column 14 line 10 and Column 17 lines 11 – 60).

Claim 36 is rejected applied as above in rejecting Claim 26. Furthermore, Baker discloses a security data packet processing wherein the processing is performed by a crypto engine and wherein subsequent to the processing, the method further comprises

prepending status information to the security protocol data packet, the status information being generated by the processing and identifying when the crypto engine detects an error (Baker Column 11 lines 15 – 27; Column 13 lines 6 – 58; Column 13 line 33 – Column 14 line 10 and Column 17 lines 11 – 60).

Claim 37 is rejected applied as above in rejecting Claim 26. Furthermore, Baker discloses a security data packet processing wherein the streaming performed when all portions of the security protocol data packet are stored second buffer (Krishna Column 5 lines 51 – 67).

Conclusion

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900 and the general central fax number is 703 – 872 – 9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
December 04, 2004.

AU2131
12/10/04